UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,828	06/07/2000	Eric J. Sprunk	D02302	9516

7590 04/05/2007

General Instrument Corporation
101 Tournament Drive
Horsham, PA 19044

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/588,828	SPRUNK ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *5* is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is written in responding to the amendment on 03/01/2006.

2. Claims 1- 5 are as original.

3. Claims 1-5 have been examined.

4. Claims 1-5 are pending.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Yorke-Smith US 5548648, cited in the Office Action dated 07/02/04.

7. As per claim 1, the limitation of encrypting information (data) by plurality of encryption keys to be sent over a communication system (e.g. message) is taught by Yorke-Smith in Column 1, lines 6-8. The limitation that the information is split into blocks (data segments) of predetermined lengths is disclosed by Yorke-Smith, Column 3, lines 25-29. Note the number L2 is generated for each segment and that determines the length of data segment, hence the length of each block is predetermined. The limitation first key K1 is used to encrypt: a data segment DS (first encrypted portion), and a second key K2 used to encrypt a data segment DS2 is taught Column 4, lines 1-2

where j = 2 . Note Figure 3 shows the break up of the data information into data segments DS, , DS2, ... DSn . Each segment being encrypted under a different key to obtain encrypted data segments EDS1 EDS2, ... EDSn The limitation that the second portion of the message overlaps the first encrypted portion of the message (see figure 3, Col 3 lines 33-40, and Col 4 lines 1-15). The CB block comprises a plurality of fields containing encrypted data block (EDS). Note that the fields of encrypted data include random numbers X which fills in between the other fields in the blocks not including the control block or the encrypted data block (Column 4, lines 54-56). Note further that the position of the encrypted data block varies dependent on the random number S. As the random numbers X that pads the encrypted data blocks (which meets the limitation of the added one or more bits of information) vary also with S and the length of the encrypted data block its L, of themselves constitute part of the encrypted data (Column 3, lines 43, 44, 45-46), the boundary between the encrypted data blocks will change relatively to the sequence of transmitted information and will thus constitutes an overlap region between the two encryption fields. Claim 1 is rejected.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith in view of Koopman, Jr. et al US 5619575, hereinafter "Koopman", cited in the Office Action dated 07/02/04.

10. As per claim 2, Yorke-smith discloses "A method for encrypting information in a message that can be authenticated, the method comprising: adding a first authentication block to the information to be encrypted to form a concatenated field" in (Col 4 lines 1-15); logically subdividing the concatenated field into predetermined block lengths, including a residual field when the concatenated field is not sized as an even multiple of the predetermined block length" in (Col 3 lines 45-55, and Figure 3); "encrypting the subdivided field using a first key to form cipher blocks" in (Col 3 lines 40-50, and Figure 3 (L1-Ln)); "designating one of the cipher blocks as a designated cipher block, the other cipher blocks being nondesignated cipher blocks; subdividing the designated cipher block into a first cipher subblock and a second cipher subblock, such that a combined length of the second cipher subblock and the residual field and a second authentication block is the predetermined block length" in (See Figure 3); "encrypting the second cipher subblock and the residual portion together with the second authentication block using a second key to form a cipher residual block" in (Col 4 lines 5-15); Yorke-Smith further teach of having control blocks (CB1-CBn) in the blocks message concerning the format of the data bytes in the encrypted data block in (Col 3 lines 33-38). However, Yorke-Smith does not disclose the control block is the authentication block and providing at least the first portion of the designated cipher

block, the nondesignated cipher blocks and the cipher residual block as the message such that the message can be authenticated by decryption of a valid authentication block of either the first authentication block or the second authentication block. Nevertheless, Koopman discloses the "Pseudorandom composition-based cryptographic authentication process" invention, which discloses an authentication block in the message to authenticate the car for entry in (Col 2 lines 29-50). It would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Yorke-smith's invention to incorporate the authentication block of Koopman to authenticate the message blocks. The authentication block would have the same functionality as the CB block in Yorke-Smith. However, it would provide the more detail information about the block to verify upon. This combination would provide authentication and integrity check of the block messages.

11. As per claim 3, the rejection basis of claim 2 is incorporated. However, Yorke-smith does not disclose the second authentication block comprises one or more bits and the second portion is less than 128 bits. Nevertheless, Koopman does mention that the authentication block can be 8 or 32 (Col 5 lines 1-10). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that the second authentication block can be incorporated and would less than 128 bits.

12. As per claim 4, the limitation that the second authentication block comprises one or more bits forming a null value (all bits zero bits). It would have been obvious to one of

ordinary skill in the art at the time that the invention was made, to have used a null value as the simplest means of validating a message. Claim 4 is rejected.

Response to Arguments

13. Applicant's amendment has Claims 1-5 as original.

14. Applicant's remark, filed on Mar. 01, 2006, argues that there is simply no discussion in Yorke-Smith which suggests "using a second key to encrypt a second portion of the message wherein the second portion overlaps with the first encrypted portion and also includes at least one bit of information in clear text", as recited by Claim 1.

15. Applicant's remark, filed on Mar. 01, 2006, argues that neither York-Smith nor Koopman, taken alone or in combination, disclose or suggest a method for encrypting information in a message that can be authenticated which includes encrypting a second cipher subblock and the residual portion together with the second authentication block using a second key to form a cipher residual block.

16. Applicant's arguments, filed on Mar. 01, 2006, have been fully considered but they are not persuasive.

Regarding to Argument (1):

Examiner respectfully disagrees with Applicant argument that there is simply no discussion in the cited reference by Yorke-Smith which suggests "using a second key to encrypt a second portion of the message wherein the second portion

overlaps with the first encrypted portion.." and also "includes at least one bit of information in clear text". Examiner has cited to Figure 3, which has the explanation in Yorke-Smith reference in Col 4 lines 1-15, which clearly describes that the encrypted block gets encrypted again by adding with the CB1... CBn, where each of the CBs comprise a plurality of fields containing information concerning the format of the data bytes in the corresponding encrypted data block EDB1... EDBn (Col 3 lines 30-40). That is, the information itself is "overlapped" with the ones in the first encrypted portion. Applicant may argue that the reference by Yorke-Smith does not teach "overlap" of the second portion of the message with the first encrypted portion based on the disclosure from the specification. However, Examiner would like to point out that the word, "overlap", is a very broad term and may be interpreted in the manner such as overlapping in the sense of having the same information bytes (i.e., data bytes reflected on the associated CB using the same encryption function and key, same padded random number X, etc.). In addition, Yorke-Smith discloses "the second portion .... includes at least one bit of information in clear text" by showing that the random numbers X, which is in the form of clear text, padded in the encrypted data block as shown in lines 43-46, Col. 3. Therefore, Yorke-Smith, contrary to Applicant's argument, clearly teaches the recited limitation "using a second key to encrypt a second portion of the message wherein the second portion overlaps with the first encrypted portion and also includes a t least one bit of information in clear text", and the rejection of Claim 1 is maintained.

Regarding to Argument (2):

In regards to Applicant's argument that neither York-Smith nor Koopman, taken alone or in combination, disclose or suggest encrypting a second cipher subblock and the residual portion together with the second authentication block using a second key to form a cipher residual block does not disclose to encrypt a cipher subblock and a residual portion together with an authentication block, Examiner respectfully disagrees. York-Smith specifically teaches that encrypting the second cipher subblock and the residual portion using a second key in lines 5-15, Col. 4, in which each subblock along with the residual block (i.e., the random padded number X) together gets encrypted with the corresponding CB1... CBn (i.e., by adding with different CBs), where each of the CBs comprise a plurality of fields containing information concerning the format of the data bytes as well as the encryption function and key in the corresponding encrypted data block EDB1... EDBn. Koopman, on the other hand, discloses an authentication block in the message and is used for the verification purpose as in lines 29-50, Col 2. The combination of York-Smith and Koopman would have the authentication block disclosed by Koopman to be incorporated with the subblock of the message along with the residual block, and the motivation to do so would be to authenticate the message blocks as suggested by Koopman in lines 44-50, Col. 2. Therefore, the combination of York-Smith and Koopman teaches the recited limitation "encrypting the second cipher subblock and the residual portion

together with the second authentication block using a second key to form a cipher residual block".

Applicant is reminded that additional modification to clarify the claimed limitation is necessary for further consideration and distinction from the prior art.

over the prior of record

Allowable Subject Matter

Claim 5 is allowable for citing a complete and detailed method on both encrypting and decrypting information in a message for authentication.

Conclusion

17. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

a. Enichen et al. (U.S. Patent 6,333,983) disclose a method and apparatus for decrypting an input block encrypted under a predetermined key in a cryptographic system having a cryptographic facility providing cryptographic functions for transforming blocks of data. The cryptographic functions include an encryption function for encrypting a block under a predetermined key and a transformation function for transforming a block encrypted under a first key to the same block encrypted under a second key. The cryptographic functions have at least one key pair with the property that successive encryption of a block under the keys of the pair regenerates the block in clear form. The input block is first transformed into an intermediate block encrypted under one of the key pair using the transformation function. The intermediate block is then further encrypted under the other of the key pair using the encryption function to generate an output block successively encrypted under the keys of pair, thereby to regenerate the input block in clear form. The invention is useful in cryptographic systems in which the decryption function being emulated by the transformation and encryption functions is unavailable for export control or other reasons.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Y.C. Shaw
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100